Gara di Gruppi 2021, Proposte di Soluzione

A Per $H < G$, indichiamo $C_H = C_G(H)$. Da $H \subset C_G(C_H)$ si deduce la prima disuguaglianza, e si verifica che vale l'uguaglianza esattamente quando $H = C_H$. Per la seconda, siano $D = H \cap K$ e $J = \langle H, K \rangle$: allora, $C_J = C_H \cap C_K$, mentre $C_H, C_K \supset C_D$. Pertanto, le disuguaglianze

$$|J| \geqslant \frac{|H| \cdot |K|}{|D|}, \quad |C_D| \geqslant \frac{|C_H| \cdot |C_K|}{|C_J|}$$

conducono a $m_G(J) \geqslant m_G(H) m_G(K)/m_G(D)$, che è quanto voluto. L'uguaglianza si verifica esattamente quando $J = HK$ e $C_D = C_H C_K$, e il punto **1.** è risolto.

Dalla seconda disuguaglianza appena provata si deduce che, posto $\mathfrak{M}(G)$ l'insieme dei sottogruppi di misura massima, questo è chiuso per intersezioni e sottogruppi generati: pertanto, possiamo prendere $N = \bigcap \mathfrak{M}(G)$, che è ancora un sottogruppo di misura massima di G. Tale N è certamente caratteristico in G, dato che gli automorfismi di G preservano m_G; inoltre, poiché per la prima disuguaglianza $\mathfrak{M}(G)$ è chiuso per centralizzatori, vale $N \subset C_N$, perciò N è abeliano. Infine, se $A < G$ è abeliano, vale $A \subset C_A$, cioè $|A|^2 \leqslant m_G(A)$, da cui per massimalità

$$[G : A] = \frac{|G|^2}{|A|^2} \geqslant \frac{|G|^2}{m_G(A)} \geqslant \frac{|G|^2}{m_G(N)} = \frac{|G|^2}{|N|^2} = [G : N]^2.$$

Il punto **2.** risulta provato.

Per il punto **3.**, notiamo che $m_G(1) = |G|$ e $|G| \mid m_G(G)$. Supponiamo per assurdo che G non sia un p-gruppo: se p, q sono primi distinti che dividono $|G|$, siano P, Q un $p-$ e un $q-$Sylow di G rispettivamente, diciamo di ordine p^a, q^b: poiché $Z(P), Z(Q) \neq 1$, vale $p^{a+1} \mid m_G(P)$ e $q^{b+1} \mid m_G(Q)$. Pertanto, $m_G(P), m_G(P) \neq m_G(1)$, e quindi tali due misure sono uguali tra loro, il che è assurdo. In conclusione, G è un p-gruppo per qualche primo p, e in particolare $Z(G) \neq 1$. D'altra parte, se $A \lneq Z(G)$, $m_G(A) = |A| \cdot |G| < m_G(Z(G))$, il che implica $m_G(A) = m_G(1)$, da cui $|A| = 1$. Perciò, $Z(G)$ è ciclico di ordine primo.

B Un gruppo G come nel punto **4.** ha $n_3 \in \{1, 7\}$, $n_5 \in \{1, 21\}$ e $n_7 \in \{1, 15\}$. Sia $S \in \mathrm{Syl}_7(G)$: se G ha un 3-Sylow P normale, PS è un sottogruppo abeliano di G, e $P < N_G(S)$, per cui 3 non divide n_7, e S è normale in G. Il discorso è del tutto analogo per un 5-Sylow Q, pertanto possiamo suppore P, Q non normali in G. In tal caso, $N_G(P)$ ha ordine 45, per cui contiene Q^x per qualche $x \in G$. Ne segue che $N_G(P) = PQ^x$, e il prodotto è diretto, dato che non esistono omomorfismi non banali $C_4 \simeq \mathrm{Aut}(Q^x) \to P$. Ma allora 3 non divide $n_5(G)$, cioè Q è normale, il che è assurdo e prova quanto voluto.

Sia ora G di ordine minimo tra i gruppi con esattamente 15 7-Sylow. L'azione di

G per coniugio su $\mathrm{Syl}_7(G)$ induce un omomorfismo $G \to S_{15}$: gli stabilizzatori dei 7-Sylow sono i coniugati $N_G(S)^x$ del normalizzatore di un Sylow S, per cui il nucleo dell'azione è il nucleo N di $N_G(S)$. D'altra parte, la mappa surgettiva

$$\mathrm{Syl}_7(G) \to \mathrm{Syl}_7(G/N),\ S \mapsto SN/N$$

è anche iniettiva, poiché $SN = TN$ implica $T \subset N_G(S)$ (dato che l'azione di N su S è banale, S è normale in SN), e cioè $T = S$; quindi G/N ha lo stesso numero di 7-Sylow di G, e per minimalità di G dev'essere $N = 1$. Pertanto, G si immerge in S_{15}; ma, dato che un elemento $x \in S \in \mathrm{Syl}_7(G)$ fissa solo S e ha ordine una potenza di 7, agisce su $\mathrm{Syl}_7(G)$ come una coppia di 7-cicli. Pertanto, A_{15} contiene i 7-Sylow di G e, per minimalità, $G = G \cap A_{15}$, cioè $G \subset A_{15}$, come voluto al punto **5.**

Notiamo adesso che un 7-Sylow S deve avere ordine 7. Dato che $S < A_{15}$, dev'essere $|S| \in \{7, 49\}$. Ora, se esistono $S, T \in \mathrm{Syl}_7(G)$ distinti tali che $S \cap T = 1$, l'equazione delle classi applicata all'azione di S su $\mathrm{Syl}_7(G)$ si legge

$$15 = 1 + \sum_T |S|/|S \cap T|$$

per certi Sylow T: preso T tale che $S \cap T = 1$, si conclude che $|S| = 7$.

Per assurdo, tutti i 7-Sylow di G si intersecano in sottogruppi di ordine p: posta $D = S \cap T$ una tale intersezione, tutti i Sylow contenuti nel suo normalizzatore $M = N_G(D)$ si intersecano in D, e $S, T \subset M$. Se allora $P \in \mathrm{Syl}_7(G)$ è un qualsiasi Sylow, $P \cap S \subset M$, per cui $P \cap S$ è contenuto in un coniugato S^x (in M) di S, da cui necessariamente $P \cap S = D$, e $S \supset D$. Questo mostra che D è contenuto nell'intersezione $O_p(G)$ di tutti i Sylow; d'altra parte, $O_p(G) \subset N = 1$, assurdo, e il punto **6.** è provato.

A questo punto, mostriamo che $|G| \mid 315$. Sia $S \in \mathrm{Syl}_7(G)$. L'azione di $N_G(S)$ su $\mathrm{Syl}_7(G) \setminus \{S\}$ lo immerge in A_{14}, e S si identifica con il generato da una coppia di 7-cicli, diciamo $S = \langle \pi \rangle$, $\pi = (1 \cdots 7)(8 \cdots 14)$. Pertanto, dall'equazione delle classi segue che $C_G(S) = S$. Inoltre, dal lemma N/C si ha $N_C(S)/S \hookrightarrow \mathrm{Aut}(S) \simeq C_6$, e si conclude che

$$|G| = [G : N_G(S)] \cdot [N_G(S) : S] \cdot |S| \mid 15 \cdot 6 \cdot 7.$$

Se però $|G| = 15 \cdot 6 \cdot 7 = 2d$, con $d = 315$ dispari, l'azione di G per moltiplicazione su sé stesso fornisce un sottogruppo normale N di indice 2 con lo stesso numero di 7-Sylow. Quindi, $|G|$ è un multiplo di $7 \cdot 15$ che divide 315: dal punto **4.** e dalla classificazione dei gruppi di ordine pqr si conclude allora che un tale G non esiste, e il punto **7.** è concluso.

C La prima identità è immediata: vale $[xy, z] = [x, z]^y [y, z]$ e l'ipotesi implice $[x, z]^y = [x, z]$. Per la seconda, procediamo per induzione scrivendo

$$
\begin{aligned}
[x^n, y][x, y] &= x^{-1}[x^n, y]y^{-1}xy \\
&= x^{-(n+1)}y^{-1}x^{n+1}y \\
&= [x^{n+1}, y],
\end{aligned}
$$

con l'altra uguaglianza del tutto analoga. Per la terza, procediamo per induzione usando la seconda,

$$
\begin{aligned}
(xy)(xy)^n &= xyx^n y^n [y, x]^{\binom{n}{2}} \\
&= x \cdot x^n y[y, x^n] y^n [y, x]^{\binom{n}{2}} \\
&= x^{n+1}y^{n+1}[y, x]^n [y, x]^{\binom{n}{2}},
\end{aligned}
$$

che conclude il punto **8.**

Per il punto **9.**, sia $A < G$ un sottogruppo di indice p: tale sottogruppo è normale, e abeliano per ipotesi. Dato allora $x \in G \setminus A$, vale $G = \langle A, x\rangle$ e, per la prima identità sopra, la mappa $\varphi : A \to G, a \mapsto [a, x]$ è un omomorfismo, ed è a valori in A poiché A è normale. Inoltre, $\operatorname{im}(\varphi) \subset G'$ ed è normale in G dato che $[a, x]^y = [a, x]$ per ogni $y \in G$: poiché $a^y = a[a, y]$, il quoziente $A/\operatorname{im}(\varphi)$ è abeliano, e $G' = \operatorname{im}(\varphi)$. D'altra parte, $\ker((\varphi)) = C_A(x) = Z(G)$, da cui si conclude

$$
|G| = [G : A] \cdot |A| = |p| \cdot |G'| \cdot [G : Z(G)].
$$

Se $B < G$ è un altro sottogruppo di indice p, $A \cap B = Z(G)$: per quanto visto, $A \cap B \supset Z(G)$, d'altra parte $G = \langle A, B\rangle$, e un elemento di $A \cap B$ commuta con entrambi A e B, quindi è centrale. Ne segue $[G : Z(G)] \geqslant p^2$ e $|G'| \leqslant p$: essendo G non abeliano, vale in effetti l'uguaglianza.

Se infine G è come in **10.**, supponiamo prima che G sia abeliano. Allora, presi $H, K < G$ distinti di ordine p, HK non è ciclico, quindi G ha un unico sottogruppo di ordine p oppure $G = HK$. Nel secondo caso, $G \simeq C_p \times C_p$, mentre nel primo G è ciclico, il che è assurdo.

Se invece G non è abeliano, scriviamo $|G| = p^n$. In questo caso, l'unico sottogruppo di ordine p è proprio G' e, per quanto visto, ogni sottogruppo di indice p contiene $Z(G)$, che è l'unico sottogruppo di ordine p^{n-2}; se quindi $A = \langle a\rangle < G$ ha indice p, $Z(G) = \langle a^p\rangle$, e più in generale G ha un unico sottogruppo di ordine p^k per ogni k tra 1 e $n-2$, generato da un'opportuna potenza di a. Mostriamo allora che dev'essere $p = 2$.

Se infatti p è dispari, la mappa $\psi_p : G \to G, x \mapsto x^p$ è un omomorfismo per la terza identità nel punto **8.** ($p(p-1)/2$ è infatti divisibile per p e G' ha ordine p), e il suo nucleo è G'; d'altra parte, ogni sottogruppo di indice p di G, essendo normale, contiene le potenze p-esime di elementi di G. Perciò, $G^p \subset Z(G)$ ha indice almeno p^2, il che è assurdo.

Infine, nel caso $p = 2$, la mappa $\psi : x \mapsto x^4$ è un omomorfismo, e la sua immagine ha indice 8 in G: dato che ogni sottogruppo di indice 2 contiene i quadrati degli elementi di G, il sottogruppo G^2 generato da tali quadrati è contenuto in $Z(G) = \langle a^2 \rangle$, e pertanto $G^4 < \langle a^4 \rangle$, da cui $G^4 = \langle a^4 \rangle$ e $[G : G^4] = 8$. In conclusione, il nucleo $N = \{x \in G \mid x^4 = 1\}$ di ψ è un sottogruppo di ordine 8, esponente 4, e con un unico elemento di ordine 2: se ne deduce $N \simeq Q_8$, e pertanto $N = G$.

Riassumendo, i sottogruppi cercati sono $C_p \times C_p$, al variare di p primo, e Q_8.

D Sia $\varphi : A \to B$ un isomorfismo. Se $A \cap \mathbf{Z} = d\mathbf{Z}$, ogni elemento di A è della forma nd/b per certi interi $n, b \in \mathbf{Z}$. Poiché φ è un omomorfismo, vale

$$b \cdot \varphi\left(\frac{nd}{b}\right) = \varphi(nd) = n \cdot \varphi(d),$$

da cui

$$\varphi\left(\frac{nd}{b}\right) = \frac{nd}{b} \cdot \frac{\varphi(d)}{d}.$$

Perciò, posto $q = \varphi(d)/d$, si ottiene che φ è della forma voluta, e il punto **11.** è provato.

Se ne deduce che, per $A < \mathbf{Q}$, $\mathrm{Aut}(A) = \{m_q \mid qA = A, q \in \mathbf{Q}\}$, dove m_q è la moltiplicazione per q. Cerchiamo allora infiniti sottogruppi di $\mathbf{Q}$ non isomorfi tali che $\mathrm{Aut}(A) = \{m_{\pm 1}\}$. Si possono ad esempio considerare, per ogni sottoinsieme $\pi \subset \mathbb{N}$ di primi positivi, i sottogruppi

$$A_\pi = \left\langle \frac{1}{p} \,\middle|\, p \in \pi \right\rangle.$$

Infatti, gli elementi di A_π sono esattamente i razionali la cui fattorizzazione ha la forma $q = \prod_p p^{q_p}$ con $q_p \geqslant -1$ per $p \in \pi$ e $q_p \geqslant 0$ altrimenti (si noti che $(q+s)_p \geqslant \min\{q_p, s_p\}$ per ogni primo p, e che se $p, q \in \pi$ allora $1/pq \in A_\pi$ per il lemma di Bézout), da cui si deduce facilmente che $m_q A_\pi = A_\pi$ se e e solo se $q \in \{\pm 1\}$.

Inoltre, due tali sottogruppi distinti, diciamo A_{π_1} e A_{π_2}, non sono isomorfi se π_1 e π_2 differiscono per infiniti primi, dato che non può esistere alcun razionale $q \in \mathbf{Q}$ per cui $qA_{\pi_1} = qA_{\pi_2}$. Questo prova il punto **12.**

E Dato che $Z(G) = 1$, la mappa $x \mapsto \gamma_x$, il coniugio per x, è un'immersione di $G \simeq \mathrm{Inn}(G)$ in $\mathrm{Aut}(G)$.

Mostriamo allora che, se $Z(G) = 1$, anche $Z(\mathrm{Aut}(G)) = 1$, provando che

$$C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1.$$

D'altra parte, nell'isomorfismo $G \simeq \mathrm{Inn}(G)$, l'azione di coniugio di $\mathrm{Aut}(G)$ su $\mathrm{Inn}(G)$

si identifica con l'azione naturale di $\mathrm{Aut}(G)$ su G: infatti, se $\alpha \in \mathrm{Aut}(G)$ e $\gamma_x \in \mathrm{Inn}(G)$, vale

$$\gamma_x{}^{\alpha}(y) = \alpha(x)^{-1} y \alpha(x) = \gamma_{\alpha(x)} \tag{1}$$

per ogni $y \in G$. Quindi, $\alpha \in \mathrm{Aut}(G)$ agisce banalmente su $\mathrm{Inn}(G)$ se e solo se $\alpha(x) = x$ per ogni $x \in G$, cioè $\alpha = 1$.

La (1) prova anche che $\mathrm{Inn}(G)$ è normale in $\mathrm{Aut}(G)$. Dato che per ogni i vale $G_i = \mathrm{Aut}(G_{i-1})$, e la dimostrazione fatta non dipende da G, il punto **13.** risulta dimostrato.

Notiamo ora che $G_{i+1} = G_i$ se e solo se G_i è completo. Per risolvere l'ultimo punto, notiamo che ad esempio $\mathrm{Aut}(A_5) = S_5$ è in effetti completo: speriamo allora che questo valga per ogni gruppo semplice non abeliano, cioè che l'N_s cercato sia 2. Vogliamo quindi mostrare che ogni automorfismo di $\mathrm{Aut}(S)$ è interno.

Sia $A = \mathrm{Aut}(S)$. Osserviamo che $S < A$ è normale per il punto precedente: d'altra parte, è semplice, e pertanto normale minimale. Mostriamo che è anche l'unico sottogruppo normale minimale di A: se $N < \mathrm{Aut}(S)$ è normale minimale diverso da S, dev'essere $S \cap N = 1$ per semplicità di S. D'altra parte, questo implica che N centralizza S (poiché N, S sono entrambi normali, vale $[N, S] \cap N \cap S = 1$), il che è assurdo. Di conseguenza, S è caratteristico in A.

Sia ora $\varphi \in \mathrm{Aut}(A)$: dato che S è caratteristico in A, l'azione di φ per coniugio su A induce un automorfismo di S, cioè coincide, su S, col coniugio per un elemento α di A. Pertanto, per ogni $x \in S$, vale $x^{\varphi} = x^{\alpha}$: questo implica che $\varphi^{-1}\gamma_{\alpha} \in C_{\mathrm{Aut}(A)}(S)$. Ma, di nuovo, questo gruppo è banale: se $C = C_{\mathrm{Aut}(A)}(S)$, vale $C \cap A = 1$ poiché $C_A(S) = 1$, e inoltre, dato che $C < \mathrm{Aut}(A)$ è normale, $[C, A] \subset C \cap A = 1$. In conclusione, $\varphi = \alpha$ è il coniugio per α, cioè ogni automorfismo di A è interno e il punto **14.** è concluso.